**Amendments to the Claims**

Please cancel Claims 1-12. Please add new Claims 13-28. The Claim Listing below will replace all prior versions of the claims in the application:

**Claim Listing**

1. Canceled

2. Canceled

3. Canceled

4. Canceled

5. Canceled

6. Canceled

7. Canceled

8. Canceled

9. Canceled

10. Canceled

11. Canceled

12. Canceled

13. (New) A process for controlling access to digital assets in a network of data processing devices, the process comprising:

defining a security perimeter that includes two or more data processing devices;

defining one or more digital asset encryption policies, to be applied to digital assets when a possible risk in use of a digital asset by an end user occurs;

sensing atomic level digital asset access events, the sensing step located within an operating system kernel in an end user client device, at a point of authorized access to the digital asset by the end user;

aggregating multiple atomic level events to determine a sequence of digital asset access events;

if the sequence of digital asset access events matches a predefined digital asset usage policy that indicates a risk of use of the digital asset outside of the security perimeter;

asserting one of the digital asset encryption policies associated with the sequence of events, by encrypting the digital asset, prior to allowing access to the digital asset from outside the security perimeter.

14. (New) A method as in claim 13 wherein the digital assets are application level data files to which the user has read and write access within the security perimeter.

15. (New) A method as in claim 13 additionally comprising the steps of:

storing the digital asset encryption policies in a policy server device in the network; and

within the operating system kernel of the end user client device,

receiving the stored digital asset encryption policies from the policy server over a secure network connection.

16. (New) A process as in Claim 13 wherein the step of asserting the digital asset encryption policy, by encrypting the digital asset prior to providing access, is implemented in an operating system kernel of the client user device.

17. (New) A method as in claim 13 wherein

the sequence of digital access events indicates that the end user is attempting to store a copy of the digital asset, and

the digital asset encryption policy specifies whether the digital asset is to be encrypted or not, depending upon a type of storage device on which the end user is attempting to store a copy.

18. (New) A method as in claim 17 wherein the encryption policy specifies that the digital asset is not to be encrypted when the type of storage device is a local file server.

19. (New) A method as in claim 17 wherein the encryption policy specifies that the digital asset is to be encrypted when the type of storage device is a removable media storage device.

20. (New) A method as in claim 13 wherein

the sequence of access events indicates that the end user is sending the digital asset through a network communication port; and

the encryption policy further specifies that the digital asset is to be encrypted, prior to sending the digital asset through the network communication point.

21. (New) A method as in claim 20 wherein

the sequence of access events indicates that the end user is attaching the digital asset to one of an electronic mail message or instant messaging service.

22. (New) A method as in claim 13 wherein

the sequence of access events includes a first file open event, followed by a clipboard copy operation, a second file open event, and a file transmit through network communication event.

23. (New) A method as in claim 13 wherein

one of the encryption policies specifies that encryption is to be applied to an asset when a particular sequence of access events is sensed; and

another of the encryption policies specifies that encryption is not to be applied to an asset when another particular sequence of access events is sensed.

24. (New) A process as in Claim 13 that operates independently of application software.

25. (New) A process as in Claim 13 additionally comprising:

determining a sensitivity level of a particular digital asset in the step of sensing atomic level digital asset access events; and

asserting one of the digital asset encryption policies by either encrypting the digital asset or not, depending upon the sensitivity of the particular digital asset.

26. (New) A process as in Claim 13 additionally comprising:

forwarding the digital asset to a second client end user device; and

asserting an encryption policy at the second client end user device.

27. (New) A process as in Claim 26 additionally comprising:

applying decryption at the second client user device.

28. (New) A process as in Claim 13 additionally comprising:

forwarding the digital asset to a second client user device; and

not asserting an encryption policy at the second client user device, so that if the encryption policy specifies encryption, the digital asset cannot be read at the second client user device.